Security analysis of Handover Key Management among 4G LTE entities Using Device Certification

B.Sridevi[1,] Divya Mohan[2]
[1,2]Dept of Electronics and Communication Engineering
Velammal College of Engineering and Technology, Madurai, INDIA

***Abstract*— The increasing popularity of wireless technologies and their application is captivating the attention of users day by day. The latest development in mobile telecommunications is the 4G architecture. LTE (long term evolution) is the candidate of next generation towards 4G in mobile broadband technology which provides a data rate of 100 Mbps and works with IP. It is a newly emerging technology and it offers enhanced speed, coverage and capacity for current mobility networks. As this is with an IP based network, ensuring network security in the course of handover is of vital importance. LTE there by presents challenges in the design of security mechanisms due to its distinctive features especially during handover. Hence in this paper, we propose an improved approach such as device certificate based key agreement among the LTE entities. The main objective is increasing the security levels between eNB and MME and the same status should be followed for MME and S-Gw, whenever UE moves from one eNB to another. In addition the proposed method for fast and secure access by key management is simulated and analysed using ns-3.**

Keywords: LTE;EPC; eNodeB; AKA; HSS; EAP; CA; Security; key management; DoS.

I. INTRODUCTION

LTE is the recently deployed standard technology for communication networks, offering higher data rates, scalable bandwidth and high peak throughputs. LTE provides wireless communication and multimedia applications such as mobile TV, video and audio streaming, internet browsing etc., The LTE system is designed to be a packet-based system containing less network elements, which improves the system capacity and coverage , and also provides seamless integration with other existing wireless networks by means of High performance. The way of achieving such performance is by implementation and supporting of handoff operations.

The major elements of the mobile LTE as shown in Fig 1 are

- User Equipment (UE) or the end user for Internet broadband Access.
- Evolved nodeB (eNB) is the only mandatory node in the radio access network (RAC) of LTE. The eNB is a complex base station that handles radio communications with several devices in the cell and carries out radio resource management and handover decisions.
- Evolved Packet Core (EPC) or Core Network deals with user authentication, access authorization and accounting (AAA), IP address allocation, mobility related signalling, QoS and security.

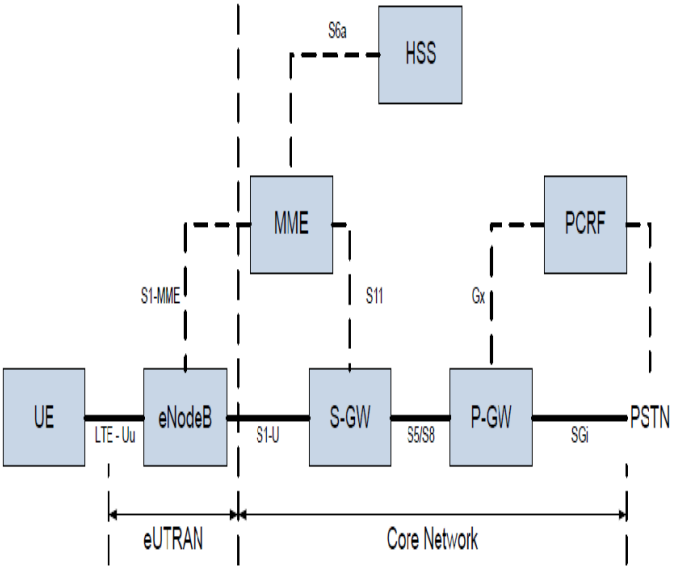

Fig. 1. Network Architecture of LTE

II. LITERATURE SURVEY

Y.Zheng, D.He et.al (2005) uses a hybrid authentication and key agreement [5] scheme to support mobility and secure communication in LTE. Here the scheme uses a dynamic password with a public key to provide a light weight authentication along with a non-repudiation service. However it may acquire lot of computational costs and storage costs. Chan-kya Han et.al (2014) [2] provides security to overcome desynchronization attacks by periodically refreshing the root key materials, but this optimal key update was not able to eradicate DoS attacks.

N.krichene et.al (2009) designed a global authentication protocol to enable a vertical handover between heterogeneous access systems [10] including

GSM,UMTS,AND WiMAX .However the handovers between LTE/LTE-A systems have not been discussed.

I.Bouabidi, I.Daly et.al (2012) introduced a new reauthentication protocol [12] for secure interworking and roaming. This scheme enhances EAP-AKA protocol and adopts a hybrid unit to offer the secure interworking.By this scheme a new entity, Hybrid Interconnection Unit (HIU), needs to be employed to serve as relay station. Between the LTE networks, which require a lot of deployment costs and changes in existing architecture.

Jin Cao et.al (2014) made a survey on the security aspects of the LTE and LTE-A networks [1] [10]. This paper discusses about an overview of security functionality of the LTE network, the security risks existing in the architecture and the existing solutions to these problems. This paper also talks about the potential research issues for the future study.

III. EXISTING METHODOLOGY

A. LTE handover Management

In LTE handover management scheme [2] the eNodeBs are making the decisions without concerning the MME due to the active mode mobility managements are circulated. The required handover information is exchanged between the eNodeBs via the X2 interface.

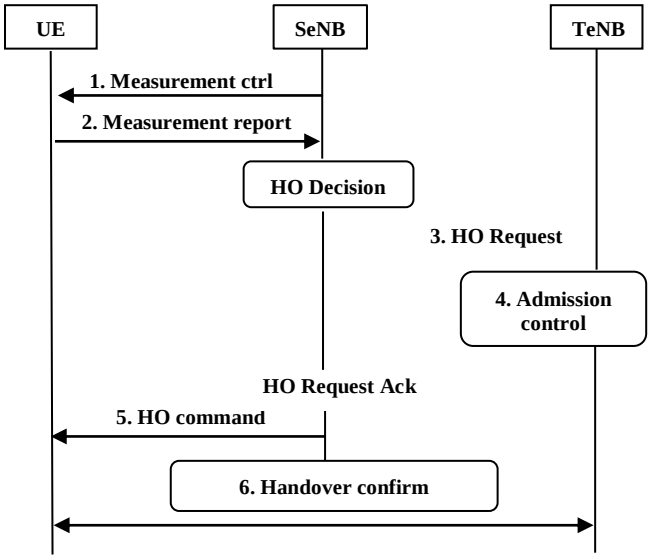

Fig. 2. Existing Handover and Key Management

The MME is informed with handover complete information after a new connection is established between UE and target eNodeB. After the reception of this information, the MME alters the path.UE is configured to do measurements and report its outcomes to the source eNodeB Figure 2. The handover procedure is activated by eNodeB based on the measurement report. The source eNodeB sends HANDOVER REQUEST message to the target eNodeB.

The target eNodeB does admission control and organizes resources (if it has adequate capacity to accept the UE). The Target eNodeB directs back the HANDOVER REQUEST ACKNOWLEDGE message.

The data forwarding is originated as soon as the source eNodeB accepts the HANDOVER REQUEST ACKNOWLEDGE to avert data loss in the course of handover. Once the HANDOVER COMMAND is received, the UE separates from the old cell, synchronizes to a new one and executes the random access procedure. The source eNodeB sends the STATUS TRANSFER message to the target eNodeB with information about the Sequence Number and the Hyper Frame Number, which the target eNodeB should allot to the first packet received from the core network (not from data forwarding).

This step offers ability to continue with in sequence delivery. The UE send the HANDOVER COMPLETE message to the target eNodeB after performing random access. Then the target eNodeB sends the PATH SWITCH REQUEST to the MME, which sends request for bearers modification to the Serving Gateway (S-GW) [7].The S-GW approves the completion of modifications to the MME and it informs the target eNodeB with the PATH SWITCH REQUEST ACKNOWLEDGE message. Finally the target eNodeB send the RELEASE RESOURCE message to the source eNodeB and the handover is accomplished.

B. Key Management

The LTE system uses AKA (Authentication and Key Agreement) for key exchange. The AKA procedure is described in the fig 3. The MME in EPC is considered to be the authenticator, but HSS is the authentication server. The authentication centre (AuC) is also present as an entity part of the HSS, which is a part of LTE architecture. The authentication scheme in 4G uses the shared symmetric authentication, which is inherited from 3G UMTS systems with some improvements. The purpose of the AKA mechanism is to create keying material for the RRC (Radio Resource Control) signalling, NAS (Non-Access Stratum) signalling and for the user-plane, both ciphering and integrity keys. The first NAS message maybe an Attach Request, PDN Connectivity or a Service Request message. This message reaches the MME, which should validate the UE's identity. If the UE is new to this network completely, then the MME inquires the UE for its permanent identity – the IMSI. This is considered a security flaw and it is not yet concentrated. On the other hand, if the UE is not new to this network, then this MME should have a GUTI in the message received from the UE.

The MME then directs the GUTI and the full TAU message to the former (old) MME, and this one replies with the accurate permanent UE identity – the IMSI and the authentication data for it. Also, if the UE roamed to this MME from a 3G network, the present MME tries to connect to the earlier management entity of this UE, and get the

IMSI information from there. If not possible, then it tries to obtain it and then connects to the HSS and validates that the IMSI that this UE uses is actually valid for this network and may have authorization to attach.

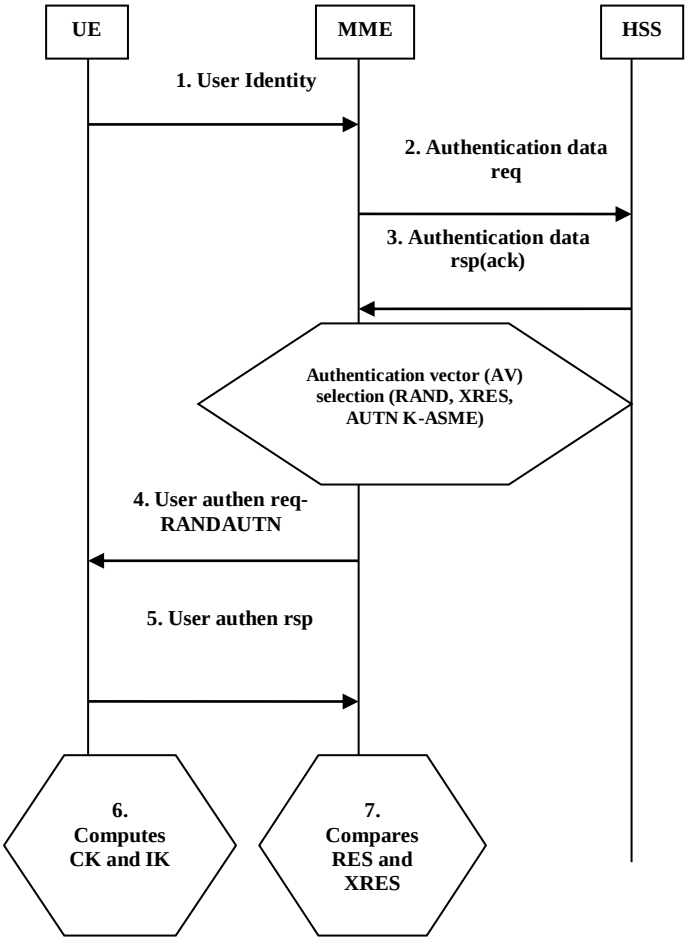

Fig. 3. LTE Key Management

The HSS receives the AV (Authentication Vector) and sends it to the MME.The HSS entity sends AVs to the MME which is presently serving the UE. The standard suggests that the HSS sends only one set of AVs, however it still sends multiple sets, so there should be a priority list which the MME should use. The UE signals in its initial message to MME and in due course access the HSS to send only the K-ASME key in the AV reply (along with AUTN , XRES and RAND), but not the CK and IK is send. Also, this K-ASME can be stored in the MME, so, when re-synchronizing the UE's status, the full AKA process may not even have to take place again. The MME sends the RAND and AUTN to the UE, then it waits for the response. Upon receipt of the message, the UE can verify, based on the AUTN, the validity of the reply, computes the RES' and sends this message to the MME. The MME verifies whether XRES Equals the RES' and if they are the same, the UE is authenticated.

TABLE 1. TERMINOLOGIES USED IN ALGORITHM

Terms	Description
UE	User Equipment
eNB	Evolved-Node B
MME	Mobile Management Entity
HSS	Home Subscriber Server
S-Gw	Serving Gateway
SeNB	Source Enb Node
TeNB	Target Enb Node
AUTH_CERT	Authority Certificate
REQ/RSP	Request/Response
CONN-REQ	Connection Request
CONN-REP	Connection Reply
CA	Certification Authority
ASME	Access Security Management Entity
AUTN	Authentication Token
RAND	Random Number
CK	Ciphering Key
IK	Integrity Key

As described, the CK and IK are computed by HSS. Also, the HSS sends initial keys to MME and eNB, which are then used by these entities to derive actual keys for NAS, user-plane and RRC traffic.

IV. PROPOSED METHODOLOGY

LTE believes that the EPC network is trusted and provides Authentication, Authorization and Accounting (AAA) connections between MME and S-Gw.

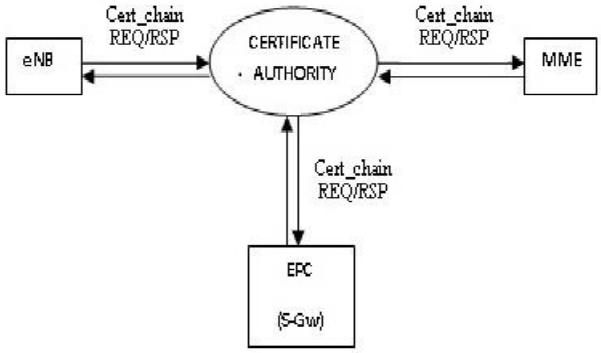

Fig. 4. Proposed Network Security

However, there are lots of possibilities for new security holes to happen including various zero-day attacks. Moreover, IPsec requires additional software and hardware facilities for supporting the whole Mobile LTE domains.

Hence, we proposed a device certificate based key exchange method which insists that all devices in LTE network should have a device certificate derived from Certificate Authority (CA) and can be verified through certificate chain.

All devices should have a certificate chain together with their own certificate as illustrated in Figure 4.The method of deriving certificate and session keys differs according to the key distribution protocols adopted by the CA. Here we use public key cryptography for deriving certificate and session keys [13] (William Stallings 2011). The proposed algorithm for the derivation of common encryption key between MME and eNB is illustrated in algorithm 1. eNB and MME should generate a secret session key in order to e**x**change messages with MME and S-Gw. For this, eNB encrypts the connection request (conn-req) message with the session key 'kenmme' padded with the timestamp (TS) and leftmost 20 bytes of Authority Certificate (Auth_cert) provided by CA. The certificates will have life time which ranges from 7 to10 days, before the certificate lifetime gets expired, the parties should request for refreshing of certificates to the CA.

Algorithm 1: For Secured Access between MME and eNB.

1. eNB and MME gets the certificate chain from CA
Cert_chain = {Auth_cert,eNB_cert,MME_cert, SGw_cert}
Msg1=E_{enmme} (conn-req) || $E_{ku\text{-}mme}$(k_{bsasn}||TS||20 bytes of Auth_cert)
eNB: Msg1 → MME
2. MME verifies timestamp & authority certificate
If valid
$D_{kr\text{-}mme}$($E_{ku\text{-}mme}$(k_{enmme}||TS || 20 bytes of Auth_cert)
Separate k_{bmme}
Conn-req=D_{kenmme} (E_{kenmme} (conn-req))
Else
Access denied
End
MME: E_{kenmme}(conn-rep || 20 bytes of Auth_cert) → eNB
3. eNB verifies authority certificate
If valid
D_{kenmme}(E_{kenmme}(conn-rep|| 20 bytes of Auth_cert))
Separate conn-rep
Else
Access denied.
End
Connection Established.

A common key would not completely protect the integrity of the message as the key shared by the user equipment can be generated by unauthenticated eNB. Consequently, in addition to the encrypted message, the session key is also encrypted with the public key of MME 'ku-mme' and padded with the message. When MME receives the message, it verifies the authority certificate and then checks the timestamp for validity.

On successful verification, MME decrypts the message and derives the key 'kenmme'. MME replies by encrypting the connection reply (conn-rep) message with the key 'kenmme', padded with the authority certificate.

Algorithm 2: For Secured Access between MME and S-Gw

1. MME and S-Gw get the certificate chain from CA
Cert_chain = {Auth_cert,eNB_cert,MME_cert,S-Gw_cert}
Msg1=E_{kmmesg}(conn- Req)|| $E_{ku=sg}$ (kmmesg)||TS||20bytes of Auth_cert)
MME: Msg1 → S-Gw
2. S-Gw verifies timestamp & authority certificate
If valid
$D_{\mathbf{kr}\text{-}sg}$ ($E_{ku\text{-}sg}$ (k_{mmesg}||TS ||20 bytes of Auth_cert))
Separate kmmesg
Conn-req= D_{kmmesg} (E_{kmmesg} (conn-req))
Else
Access denied
End
S-Gw:E_{kmmesg} (conn-rep || TS||20 bytes of Auth_cert) → MME
3. MME verifies authority certificate
If valid
D_{kmmesg}(E_{kmmesg} (conn-rep|| TS||20 bytes of Auth_cert))
Separate conn-rep
Else
Access denied
End.
Connection Established.

Similarly to S-Gw, 'kmmesg' is generated as a common encryption key .Thus the secret session key eliminates the insecurity existing between eNB-MME and MME-S-Gw. Hence a secure communication is established. This methodology can also be adopted for communication between eNBs. During handoff, all message exchanges between UE and Target eNB (TeNB) are done through the Service eNB (SeNB). To avoid security threats, a common encryption key 'ksenten' is derived similar to 'kenmme' and 'kmmesg' and is detailed by the proposed algorithm, communication between SeNB and TeNB can be made trustworthy.

The proposed work minimizes the probability for MITM attack, Masquerade and Denial of Service (DoS) attack. Since the device certificate serves robustly for verifying the authenticity, timestamp ensures the validity of the message and public key encryption ensures confidentiality. On the whole, this proposed approach ensures a secure access network communication in the LTE network at the cost of additional resources and time delay.

Algorithm 3: For Secured Access between SBS and TBS

1. SeNBand TeNB get the certificate chain from CA

Cert_chain= {Auth_cert,eNB_cert,MME_cert, S-Gw_cert}
Msg1=$E_{ksenten}$ (conn-req) ||E_{ku-sg} (k_{senten}|| TS||20 bytes of Auth_cert)
SeNB: Msg1 →TeNB
2. S-Gw verifies timestamp & authority certificate
If valid
D_{kr-sg} (E_{ku-sg} (k_{senten} ||TS ||20 bytes of Auth_cert)
Separate k_{senten}
Conn-req= $D_{ksenten}$ ($E_{ksenten}$ (conn-req))
Else
Access denied
End
TeNB:$E_{kssenten}$ (conn-rep|| TS||20 bytes of Auth_cert) →SeNB
3. SeNB verifies authority certificate
If valid
$D_{ksenten}$ ($E_{ksenten}$ (conn-rep|| TS||20 bytes of Auth_cert))
separate conn-rep
Else
Access denied
End
Connection Established.

V. SECURITY ANALYSIS USING NS-3

The Algorithm is simulated using NS-3. The proposed work insists the importance of secured communication between the entities of LTE like UE, MME and S-Gw by a device based certificate generation. And this simulation is analyzed for DDOS attacks. DDOS attacks is comprised of several other multiple attacks. As LTE is considered to be a IP based network there is a higher possibility of attacks such as SYN floods , UDP floods , ICMP floods, fragmented packet attacks and zero day DoS attacks If DDoS attacks have been mitigated then there is a possibility of eradicating the above mentioned attacks. First a LTE model was created in NS-3 as shown in Fig 5, here in case of LTE, since the authentication is based on device certificate, each user holds the certificate chain as shown in Fig 5, already issued by CA from which each user and entity can verify the authenticity of other users and entities. The device certificate includes serial number, the identity of the issuing authority, user identity, public key of the entity, digital signature of the entity and the cryptographic algorithm used together with its parameters. Whenever a request or response is received by any entity, say A, from another entity, say B, this certificate pool is traversed to check whether the received certificate of B is exactly the same as the one issued by CA. Only the message with the correct certificate padded will be processed and replied for further connection in the network.

Fig 4, represents the for the proposed access network security between BS and ASN-GW. AUTH_CERT represents the device certificate used for the authentication of the entities. 'TIMESTAMP' represents the validity usually current clock time is used to avoid replay attacks. 'REQUEST' includes the connection request from BS to

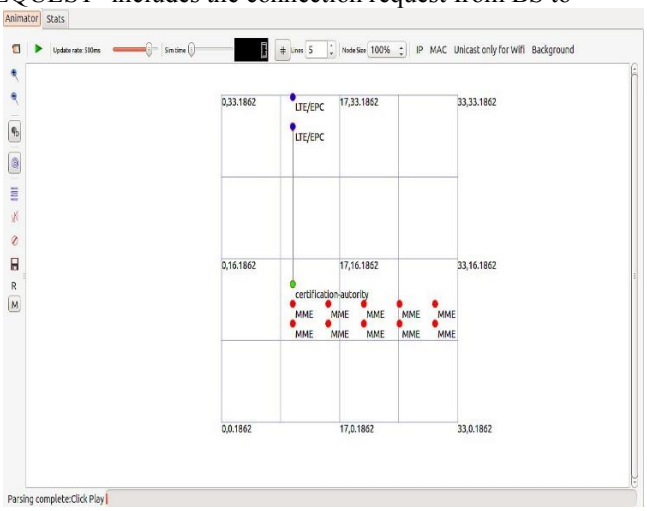

Fig. 5. LTE model and secured access between LTE entities.

ASN-GW. It includes the connection request which indicates the management messages between the entities.

'REQUEST' also includes encrypted form of 128 bit KBSASN key by 64 bit public key of ASN-GW, leftmost 20 bytes of authority certificate and time stamp other than connection request.'RESPONSE' indicates the encrypted reply by an entity which includes the connection reply and the device certificate as shown in Fig 6.After the successful mutual verification of MME and eNB, further communication messages between these entities are encrypted with the keys. The encryption technique used here is AES-128.[13] [12].The common encryption key or session key is generated between the entities for security. Secured
Communication between SeNB and TeNB during the handoff also requires a similar process to derive a session key between them.

TABLE 2. LTE Model parameters for security analysis

Parameters	Value
Simulation time	9.999 s
Round trip time(rtt) min	7s
Rtt average	4.925 s
Nodes created	10
Packets transmitted	10
Packets received	9
Packet loss	10%

The proposed device certificate based access between entities ensures the assurance for security between the

entities. Device certificates should be updated periodically to enhance long term security.

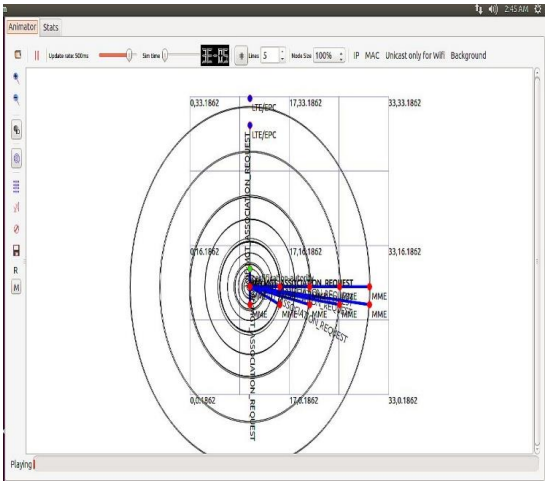

Fig. 7. Connection establishment of LTE entities

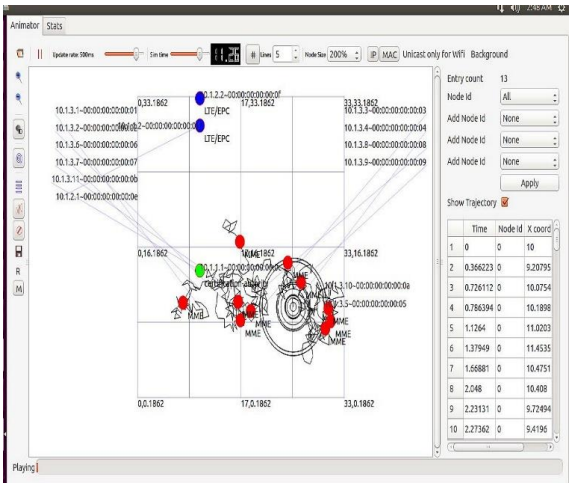

Fig. 8. Analyzation of DDoS attack

VI. CONCLUSON AND FUTURE ENHANCEMENT

Last decade research in wireless networks gave more importance to speed rather than security. This paved the way for the increase in security threats which spoils the network and attempted to make the communication as disclosure. The main contributions in the security of communication between LTE network entities are resolved by the usage of proposed device certificate chain among the entities like eNB, MME and S-Gw to generate a shared session key called pre-TEK. Further enhancement of security during service establishment from S-Gw to UE is done. (i.e) service security is also provided in addition to secure handover. Some of the limitations of this proposed work are time and bandwidth constraints. With the focus of providing efficient security these constraints can be compromised but still they induce to improve the proposed work as future enhancement.

REFERENCES

[1] Jin Cao, maode ma, IEEE Hui li, Yueyu Zhang and Zhenxing luo: "A survey on security aspects for LTE and LTE-A networks", *IEEE Communications Surveys & Tutorials*., VOL.16, May 2014.

[2] chan-kya Han and hyoung-kee choi,"Security Analysis Of Handover Key Management In 4G LTE/SAE Networks", *IEEE Transactions on Mobile Computing* ,VOL.13 , NO.2, FEB 2014.

[3] Mohsen M.Tantaway, Adly S.Tag Eldein and Esraa Mosleh Eid:"Performance Analysis of Multicast Security in LTE", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, VOL.2, ISSUE 5, Sept-Oct 2013.

[4] Anand R.Prasad and Xiaowei Zhang:,"Overview Of LTE/SAE Security",*IEEE Transactions On Smart Processing And Computing.*,vol.2,no.1,February 2013.

[5] Khaled Y.Yousef, Heshman Kamel ,Ahmed A. Hafez and Abdel Halim A.Zerky:"On Balance Between Security And Performance For LTE Wireless Networks" ,*International Conference On Computing : Theory And Applications (ICCTA)*, Paris, France ,October 2012.

[6] Y. Zheng, D. He, L. Xu, and X. Tang:"Security Scheme for 4G Wireless Systems" *Proc. Communications, Circuits and Systems, pp.* 397- 401, May 2005.

[7] Dan Forsberg, Ganther Horn, Wolf-Dietrich Moeller and Valtteri Niemi:"LTE Security",*John Wiley & Sons* Ltd,2010.

[8] D.Astely, E. Dahlman, A. Furuskar, Y. Jading, M.Lindstrom, and S. Parkvall:"LTE: The Evolution of Mobile Broadband"*IEEE Communications Magazine*, pp.44-51, April 2009.

[9] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas:"LTE-advanced: Next-generation Wireless Broadband Technology", *IEEE Wireless Communication*, pp.10-22 June 2010.

[10] Y. Park and T. Park:"A Survey of Security Threats on 4G Networks", *IEEE Globecom Workshops*, pp.1-6, November 2007.

[11] N. Krichene and N. Boudriga:"Securing Roaming and Vertical Handover in Fourth Generation Networks" *Proc. Network and System Security (NSS '09)*, pp.225-231 October 2009.

[12] I. Bouabidi, I. Daly, and F. Zarai,"Secure Handoff Protocol in 3GPP LTE Networks", *Proc. Third International Conference on Communications and Networking (ComNet)*, pp.1-6, March 2012.

[13] X. Li, and Y. Wang,"Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network", *'Proc. Wireless Communications, Networking and Mobile Computing (WiCOM)*, pp.1-4, Septmber 2011.

[14] "Cryptography and Network Security" *'William Stallings*, Pearson Education, 2007